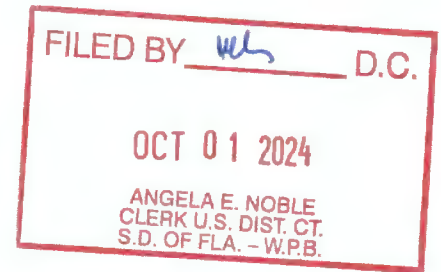


**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF FLORIDA**



**JEFFREY BUONGIORNO,**

Plaintiff,

v.

Case No. 9:24-cv-80920-AMC

**ALEJANDRO MAYORKAS, et al**

**PLAINTIFF'S MOTION FOR TEMPORARY RESTRAINING ORDER AND  
INJUNCTIVE RELIEF**

Plaintiff, moves this Honorable Court for a Temporary Restraining Order (TRO) and Injunctive Relief to immediately halt the use of the voter registration contractor VR Systems due to significant cybersecurity threats and violations of Florida law, particularly Fla. Stat. §98.035.

Plaintiff requests that the Court enjoin the Defendants from using VR Systems in the election process and halt the counting of mail-in ballots due to these ongoing cyber threats. In support of this motion, Plaintiff states as follows:

---

## **FACTUAL BACKGROUND**

### **1. Unlawful Use of Outsourced Voter Registration Contractor**

Pursuant to Fla. Stat. §98.035, the Florida Department of State is required to ensure the security and integrity of voter registration systems. VR Systems, an outsourced contractor, was unlawfully engaged without proper safeguards, in violation of state and federal law.

### **2. Cybersecurity Threats and 2016 Russian Hack**

VR Systems was directly compromised in a cyberattack in 2016, perpetrated by Russian actors, leading to the unauthorized breach of sensitive voter data. This breach underscores the vulnerability of the system and its continued use presents an ongoing threat to the integrity of future elections.

### **3. Cyber Outages in the August 20, 2024, and August 23, 2022 Primaries**

In addition to the 2016 breach, VR Systems experienced significant cyber outages during the August 20, 2024, and August 23, 2022 primaries, further demonstrating its vulnerability and the risk it poses to the election process. These outages disrupted voter registration and ballot processing, casting serious doubts on the reliability of the system and the integrity of the results from those elections.

### **4. Threat to Mail-In Ballot Processing**

The cybersecurity risks also extend to the processing of mail-in ballots. VR Systems' vulnerabilities place the integrity of mail-in ballot counting at serious risk, which could lead to

manipulation or unauthorized access by malicious actors. Due to this threat, the counting of mail-in ballots must be immediately halted until proper security measures are implemented.

#### **5. Evidence of Time-Stomping and Cybersecurity Vulnerability in Public Records**

The EL45A report from the Palm Beach County Supervisor of Elections shows clear evidence of time-stomping, which exposes an additional cybersecurity threat vector. This evidence was revealed through the response to a public records request (PRR) but was improperly concealed when the county altered public records request #23-42 to cover up this vulnerability.

#### **6. Alteration of Public Records and Tampering**

Not only has Palm Beach County altered public records, but the State of Florida has also manipulated data on its public portal for candidates, specifically the website:

<https://countyballotfiles.floridados.gov/votebymymailvotingreports/>. **Exhibit P13** demonstrates tampering and irregularities with the data, further compromising the integrity of the election process.

#### **7. Unlawful Implementation of Rule 2.027 and Concealment of Public Records**

The State unlawfully implemented Rule 2.027, removing two critical fields from the DS-DE 40 form, which obscures the reporting of blank ballots and duplicated ballots. The rule allows the Canvassing Board to adjudicate ballots based on "voter intent" via Form DS-DE 420, a clear violation of public transparency laws and a concealment of public records.

**Exhibit P9** provides documentation from the Canvassing Board meeting on August 9, 2024, where Defendant [INSERT NAME] seconded the motion to adopt Rule 2.027, directly



contributing to the unlawful rule change. This change resulted in the removal of critical fields from Form DS-DE 40, which subsequently undermined transparency in the election process.

**Exhibit P14** includes an email dated September 26, 2024, where Defendant [INSERT NAME] claimed they were not a member of the Canvassing Board, demonstrating an inconsistency in their role and actions.

#### **8. Masquerading Blank Ballots and Duplicated Ballots**

The EL52A report from the 2022 General Election in Palm Beach County (**Exhibit P10**) shows 59 blank ballots, further supporting the Plaintiff's claim that the state is attempting to obscure the reporting of blank ballots and duplicated ballots through the unlawful changes made under Rule 2.027. This manipulation of election records undermines transparency and violates Fla. Stat. §98.035, which mandates the maintenance of accurate and secure election data.

#### **9. VR Systems Terms and Conditions Holding Them Harmless for Data Breaches**

**Exhibit P15** includes VR Systems' terms and conditions, which explicitly hold them harmless in the event of a data breach. This provision underscores the irresponsibility of continuing to use VR Systems in the election process. Despite the significant cybersecurity risks posed by the company, including its previous compromise in 2016, the terms shield VR Systems from liability, further jeopardizing the security and integrity of the election process.

#### **10. Domain Hosting Election Night Results Also Maintained by VR Systems**

Further aggravating the risks, VR Systems also maintains the domain **electionsfl.org**, which is responsible for hosting election night results. This domain is subject to similar cybersecurity

threats as the VR Systems domain and poses an additional vulnerability to the transparency and accuracy of election results. The failure to secure this domain could lead to manipulation or unauthorized access, further eroding public confidence in the election process.

#### **11. Plaintiff Buongiorno's Evidence Delivered to the Canvassing Board**

Plaintiff **Buongiorno** presented evidence to the Palm Beach County Canvassing Board on **March 14, 2023**, and **July 2, 2024**, during official meetings. This evidence, which is directly relevant to the claims regarding cybersecurity vulnerabilities and improper election processes, was recorded and published on the county's official YouTube channel. This public dissemination further supports the transparency of the claims and provides documented proof of the issues raised by the Plaintiff before the board.

#### **12. Cybersecurity Assessment of electionsfl.org Domain**

**Exhibit P16** contains a comprehensive cybersecurity assessment report for the domain **electionsfl.org**, which was conducted using advanced tools including NMAP, AlienVault, Robtex, Shodan, and Maltego. The report details the specific vulnerabilities and cybersecurity risks associated with this domain, which is critical for hosting election night results. The findings reveal significant weaknesses that expose the domain to potential cyberattacks, data breaches, and manipulation, further jeopardizing the integrity of the election process.

#### **13. Cybersecurity Assessment of VRSYSTEMS.com Domain**

**Exhibit P17** includes the cybersecurity assessment report for the **VRSYSTEMS.com** domain, using the same industry-standard tools such as NMAP, AlienVault, Robtex, Shodan, and



Maltego. The assessment outlines the serious security vulnerabilities of the VR Systems domain, confirming the high risk of cyberattacks and data breaches, which threatens the overall security of the election systems managed by VR Systems. This report underscores the critical need for immediate action to secure the election infrastructure.

**14. VR Systems Memo Regarding August 20, 2024 Primary Election Outage**

**Exhibit P18** is a memo dated **August 21, 2024**, from VR Systems, issued the night after the primary election results went down due to a significant outage. In this memo, VR Systems announced that they were hiring third-party investigators to look into the outage. However, as of the date of this motion, no public statement or report has been released regarding the findings of this investigation, further raising concerns about the transparency and integrity of the election process.

**15. Defendant Link's Admission Regarding VR Systems' Operations on September 25, 2024**

On **September 25, 2024**, during a debate at **Palm Beach State College**, which was live-streamed by **WKTV** and hosted by local anchor **Michael Williams**, **Defendant Link** admitted that **VR Systems** was responsible for handling Florida's voter roll registrations. This public acknowledgment further confirms VR Systems' involvement in critical election operations, raising significant concerns given their history of cybersecurity vulnerabilities. Despite this admission, no additional measures have been publicly disclosed to secure voter roll systems.

**16. Likelihood of Third-Party NGOs Ordering Mass Numbers of Vote-by-Mail Ballots**

There is a **high likelihood** that third-party **NGOs** (Non-Governmental Organizations) have ordered mass numbers of vote-by-mail ballots based on voter registration data they have harvested through various means. This practice undermines the integrity of the election process and places voter data at risk. Given this significant threat, Plaintiff requests as injunctive relief that the **State of Florida** and its contractors be prohibited from withholding the **originating IP addresses** of vote-by-mail requests. During the **September 25, 2024 debate**, **Defendant Wendy Link** stated that she would never release the IP addresses, relying on misleading or untruthful information to justify withholding this critical data.

#### **17. Buongiorno's Public Records Request for Vote-by-Mail IP Addresses**

**Exhibit P19** reflects that **Defendant Buongiorno** has placed a public records request with the Palm Beach County Supervisor of Elections, asking for the originating IP address of his own vote-by-mail request. Despite this personal request, Buongiorno reasonably anticipates that the request will be denied, highlighting the County's refusal to release even personal information that poses no security risk.

#### **18. Intimidation of Citizens Through Signature Challenges**

**Exhibit P20** contains a letter from the Palm Beach Supervisor of Elections' attorney accusing a citizen of committing a crime for challenging too many voter signatures. The signatures in question evidenced a **high likelihood of digital manipulation**, raising concerns about the integrity of the verification process. The ability to generate manipulated signatures in large volumes represents a serious threat to election security. This accusation is yet another tactic of

**intimidation** employed by the County to dissuade citizens from raising legitimate concerns regarding election integrity.

#### **19. Defendants Conspiring to Manipulate the Outcome of the 2024 General Election**

There is substantial evidence to support the claim that **Defendants Wendy Link, Maria Marino, and Robert Weiss** are **conspiring to manipulate the outcome of the 2024 General Election**. Their actions, as detailed in the evidence provided, including tampering with public records, unlawful changes to Rule 2.027, and deliberate obstruction of transparency regarding vote-by-mail requests, point to a coordinated effort to undermine the integrity of the election process. Their involvement in manipulating the results should disqualify them from participating in the November 2024 General Election. The **Plaintiff requests** that Defendants Link, Marino, and Weiss be **enjoined** from any participation in the election to prevent further manipulation and protect the public's right to a free and fair election.

---

### **LEGAL ARGUMENT**

#### **20. Violation of Fla. Stat. §98.035**

Under Florida law, it is mandatory that voter registration systems are secure and maintain integrity. The ongoing use of VR Systems, given its prior compromise in 2016 and its outages during the 2022 and 2024 primaries, constitutes a violation of this statute. The continued use of such a system poses a substantial risk to the security of voter data and election integrity.



## **21. Civil Voting Rights Will Likely Be Violated**

Failure to halt the use of a compromised system such as VR Systems threatens to violate the civil voting rights of citizens. The integrity of the voting process is paramount in ensuring equal protection under the law. Allowing the ongoing use of a system that is vulnerable to cyberattacks, which has already led to improper counting of blank and duplicated ballots, disproportionately affects voters by diluting their votes and undermining the fairness of the election. These violations constitute a direct threat to the fundamental civil rights guaranteed by the U.S. Constitution, including the right to vote free from interference and manipulation.

## **22. VR Systems' Lack of Accountability for Data Breaches Constitutes a Clear Risk**

The terms and conditions of VR Systems, which hold the company harmless in the event of a data breach (Exhibit P15), further exacerbate the risk to election security. The State's reliance on a vendor that is not accountable for safeguarding voter data poses an ongoing and substantial threat to the integrity of elections. This lack of accountability highlights the need for immediate injunctive relief to protect the public interest and the election process from further harm.

## **23. Domain electionsfl.org Maintained by VR Systems Poses Additional Risks**

The **electionsfl.org** domain, which is also maintained by VR Systems and hosts election night results, is subject to similar cybersecurity vulnerabilities as VR Systems' other domains. This presents a clear and present danger to the integrity of election reporting, as any breach or manipulation of election night results could severely undermine the public's trust in the election outcome.

#### **24. Civil Rights Threatened by Withholding IP Addresses of Vote-by-Mail Requests**

The refusal to release **originating IP addresses** of vote-by-mail requests, as admitted by **Defendant Link** on **September 25, 2024**, further undermines election transparency. With the growing likelihood that third-party NGOs have harvested voter data and ordered mass numbers of vote-by-mail ballots, this information is critical for election integrity. Withholding these IP addresses raises serious concerns about fraudulent activity in the vote-by-mail process.

#### **25. Intimidation Through Criminal Accusations for Signature Challenges**

The **intimidation of citizens** through legal threats for challenging signatures, as demonstrated in **Exhibit P20**, constitutes another form of suppression and undermines public trust in the election process. The signatures challenged showed evidence of **digital manipulation**, indicating systemic problems in the verification of signatures. Rather than addressing these issues, the County has chosen to threaten legal action against citizens, further jeopardizing the transparency and fairness of elections.

#### **26. Defendants Link, Marino, and Weiss Conspiring to Manipulate Election**

The evidence presented demonstrates that **Defendants Link, Marino, and Weiss** are actively conspiring to manipulate the outcome of the 2024 General Election. Their coordinated efforts to obstruct transparency, alter records, and suppress valid challenges to election integrity represent a serious threat to the democratic process. These actions should disqualify them from further participation in the 2024 General Election. **Plaintiff requests injunctive relief** to enjoin Defendants Link, Marino, and Weiss from any further involvement in the November 2024

General Election, ensuring the integrity of the electoral process and protecting the public's right to a free and fair election.

**27. Cybersecurity Threats Constitute Irreparable Harm**

The Plaintiff demonstrates a real and imminent threat of irreparable harm, as the continued use of VR Systems and the counting of mail-in ballots via a compromised system jeopardizes the entire election process. Once the election results are tainted, there is no adequate remedy at law, necessitating immediate injunctive relief.

**28. Public Interest and Balance of Equities Favor Injunctive Relief**

The public's interest in a secure and transparent electoral process far outweighs any potential inconvenience to the Defendants. Immediate injunctive relief is necessary to protect the public's right to a free and fair election.

---

**PRAYER FOR RELIEF**

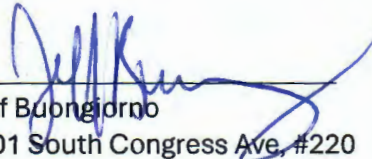
WHEREFORE, Plaintiff respectfully requests that this Court:

1. Grant a Temporary Restraining Order immediately halting the use of VR Systems in processing voter registration and mail-in ballots due to the cybersecurity threats.



2. Enjoin the Defendants from counting any mail-in ballots processed through VR Systems.
3. Order the immediate halt of the implementation of Rule 2.027 and restoration of the removed fields in Form DS-DE 40.
4. Order full transparency and the release of all records regarding the time-stomping and cybersecurity vulnerabilities, including full compliance with public records requests (Exhibits P5-P20), and the release of **originating IP addresses** for all vote-by-mail requests.
5. Enjoin Defendants Wendy Link, Maria Marino, and Robert Weiss from any participation in the November 2024 General Election due to their conspiracy to manipulate the election process.
6. Provide such other relief as this Court deems just and proper.

Respectfully submitted this First day of October, 2024.



Jeff Buongiorno  
1901 South Congress Ave, #220  
Boynton Beach, FL 33426

---

## EXHIBITS

- **Exhibit P5:** Minutes of the August 9, 2024 Canvassing Board Meeting.